DECLARATION UNDER 37 C.F.R. §1.131 AND EXHIBITS

JUN 2 3 2005 C

CERTIFICATE OF MAILING/TRANSMISSION (37 C.F.R. 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING
deposited with the United States Postal
Service, with sufficient postage, as first class mail
in an envelope addressed to the Commissioner for
Patents, P.O. Box 1450, Alexandria, VA 223131450

FACSIMILE

transmitted by facsimile to the Patent and Trademark Office.

Date: 20 June 2005

Signature
Lisa L. Pringle

(type or print name of person certifying)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:) \
Kenneth W. Aull) Group Art Unit: 2133
Serial No.: 10/027,607))
Filed: December 19, 2001) Examiner: Nadia Khoshnoodi
Ear Bublic Ven Infrastructure Token Issuan	ce and Binding

DECLARATION UNDER 37 C.F.R. §1.131

Sir:

I, the undersigned, declare as follows:

- 1. I, Kenneth W. Aull, am an inventor of the invention entitled Public Key Infrastructure Token Issuance and Binding, disclosed and claimed in U.S. Patent Application Serial No. 10/027,607 (hereinafter to as "the Application"), which was filed on December 19, 2001.
- 2. I along with my co-inventors, Thomas C. Kerr, William Freeman and Mark A. Bellmore, conceived the subject matter that is disclosed and claimed in the Application prior to December 20, 2000, while employed for a predecessor-in-interest to the Assignee.

- 3. Prior to December 20, 2000, I prepared a written description in the form of a PowerPoint® presentation of various aspects of a PKI architecture, including the subject matter claimed in the Application. The written description was updated on November 9, 2000, presenting evidence that the subject matter was conceived at least prior to November 9, 2000. A copy of this written description is attached hereto as Exhibit A.
- 4. On January 4, 2001, I completed a second written description in the form of a PowerPoint® presentation of various aspects of a PKI architecture, including the subject matter claimed in the Application. A copy of this second written description is attached hereto as Exhibit B.
- 5. On February 19, 2001, we submitted an invention disclosure relating to the application. A redacted copy of the invention disclosure is attached hereto as Exhibit C.
- 6. On April 5, 2001, a letter from Lorna Schott (Patent Administrator for the Assignee) requesting preparation of a patent application was forwarded to Donald E. Stout, Esq. at the law firm of Antonelli, Terry, Stout & Kraus, LLP. The letter included the disclosure for the invention described in the Application under docket number 15-0254. A redacted copy of the letter is attached hereto as Exhibit D.
- 7. On Wednesday, April 11, 2001, Henry M. Zykorie at the law firm of Antonelli, Terry, Stout & Kraus, LLP sent an email to me that included a request of additional information. A copy of the email is attached hereto as Exhibit E.
- 8. On Thursday, May 3, 2001, Thomas C. Kerr sent an email to Henry M. Zykorie that included the information requested in Exhibit E. A copy of the email is attached hereto as Exhibit F.

- 9. On June 22, 2001, Henry M. Zykorie sent a letter to Lorna L. Schott that included a draft of the Application, which was prepared by the law firm of Antonelli, Terry, Stout & Kraus, LLP. A copy of the letter is attached hereto as Exhibit G.
- 10. After a review of the draft of the Application, on October 18, 2001, a letter including a marked up copy of the draft of the Application was sent to Henry M. Zykorie of the law firm Antonelli, Terry, Stout & Krous, LLP. A redacted copy of this letter is attached hereto as Exhibit H.
- 11. On October 26, 2001, another draft of the Application was included in a letter to Lorna Schott from Henry M. Zykorie. A copy of this letter is attached hereto as Exhibit I.
- 12. I believe that the Application was filed in the U.S. Patent Office on December 19, 2000.
- 13. I declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Kenneth W. Aull

Date

June 16, 2005

TABLE OF CONTENTS

	Ехнівіт
CONCEPT OF INVENTION (11/09/2000)	A
SECOND WRITTEN DESCRIPTION 01/04/2001)	В
Invention Disclosure (02/19/2001)	C
INVENTION FORWARDED TO COUNSEL (04/05/2001)	D
EMAIL FROM COUNSEL REQUESTING ADDITIONAL INFORMATION (04/11/2001)	Е
Email to Counsel Including Requested Information (05/03/2001)	F
DRAFT OF APPLICATION TO ASSIGNEE (06/22/2001)	G
Changes Forwarded to Henry M. Zykorie (10/18/2001)	Н
SECOND DRAFT OF APPLICATION TO ASSIGNEE (10/26/2001)	I

The Winning Technical Strategy Class 4 PK

Ken Aull

11/9/2000

TRW Proprietary

DoD Class 4 PKI A complex Customer set (8)



□ Many Oars are in this water

- Sponsor of the project has directed that the players below be nice or lose their money
- Class 4 Program Office
- » Program Manager -
- is the customer for the system. They run the Class 3 system, which by direction Class 4 system will be replaced with the
- · Common Access Card (CAC) Program
- Run by the grant a forced marriage with the Class 4 PKI
- **Global Information Grid**
- These people supply the Directory technology for the DoD
- A and the KMI initiative (Key Management Initiative)
- will evaluate the security They see this as funding for their KMI program
- Have the bulk of the money 22 Independent Agencies of the
- Users Not represented by anyone but the prime integrator

What is the winning technical strategy?



□ TRW Enterprise Directory and Security (TEDS)

- Not the solution for the without significant modification
- **TEDS depends on Apriori Authoritative sources**
- policy defines users post facto
- TEDS depends on a well defined management structure
- Chain-of-Command not well suited to this requirement
- TEDS assumes a reasonable level of paranoia about security
- » Technical evaluation team defines new heights of "what if" paranoia

What TRW brings is an uncommon concern with

- High Security
- **Low Cost**
- Strictly enforced processes and procedures
- · Replaceable COTS structures
- » Have used both Netscape and E-Certify

The Local Registration Authority (LRA)

TRW

□ The LRA is the Achilles Heel of PKI

- · A Classic LRA costs 1 full head per 2000 users
- ☐ TEDS eliminated the LRA
- The manager became the Face-to-Face agent
- Elimination of the LRA in the is not possible
- The CAC officer is the LRA a given
- There is no authoritative source for manager
- One of the constituents is the CAC program
- » Will not look favorably on being eliminated
- □ Many of the 22 agencies (for example)
- · Will have their own badges
- Need to be incorporated into the process
- These are an unfunded liability to the program

CLASS 4 Operations - an opportunity

TRW

- Class 4 implies a hardware token
- The hardware token opens the opportunity for TRW
- Keep the CAC operators, but add no PKI overhead
- Easily add badging operators from 22 Agencies
- Eliminate cost of LRA function to support PKI
- ☐ The TRW primary Golden-Goo-Goo (G³)
- Make the CAC operator a badging operator (as intended)
- CAC operator does no explicit LRA functions
- · User visits CAC only for badging functions
- To obtain the first badge
- » To get a loaner badge for a temporary displacement
- » To get a replacement badge for a lost badge
- » To return a badge during check-out

The TRW CONOPS

TRW

□ TRW concept is for an "invisible" LRA

- Functionality is hidden from the badging officer and user
- Badging officer does standard functions
- Identifies User via paper process
- Checks against "database" of users (e.g. Deers/Rapid for CAC)
- Checks for existing badge (Class 4 keeps record)
- Creates badge, including picture, fingerprint, and PKI certificate
- Allows user to create a PIN for the badge
- » Signs the badge out to the user (Face-to-Face)
- Cancels any lost badge
- Issues temporary badges, logs and destroys returned badges
- From the view point of the user and the badging officer
- PKI appears to add no additional complexity
- Common that is done, no further action required, ever
- No additional labor over issuing a plastic badge as currently done
- » User never revisits the LRA for ANY PKI related reason
- » No labor expended for the support of PKI TRW PROPRIETARY

TRW CONOPS

TRW

☐ Simple user visits badging office for a badge

- · User comes away with a badge
- » Picture for humans
- » Digital Signature for computers and documents
- If badge is lost or expires
- Returning to the badge office restores picture and Digital signature
- » Cancels (revokes) any private key stored on token
- Temporary badge creates a one-day signature
- Does not require canceling the permanent badge or certificate
- » No flooding of the Certificate Revocation List (CRL)
- Returned badges only require physical destruction of badge
- Physical destruction eliminates any chance for use
- » Does not require flooding of the Certificate Revocation List (CRL)

TRW

□ Office worker will require Encryption certificate

- TRW approach allows remote generation of encryption keys
- The private key can only be unlocked on the token (G3)
- The identity of the User and Badge is crytologically sound (G³)
- The function happens on an untrusted workstation (G3)
- » Removes the labor of visiting the badge office
- » Travel, badge officer time, user time are all saved

□ Recovery of Encryption certificate is the same

- User uses token for identification
- User recovers directly the encryption certificate and keys (G³)
- Keys are never exposed to the untrusted Workstation (G3)

TRW

□ Organizations will require Role Certificates for users

- Roles are created by TRW E-Form Process (G3)
- Roles members are managed by Role Owner identified in Form (G3)
- Process is entirely electronic, and definable by Sponsor (G3)
- Greatly simplifies the day to day management of KMI

Users will require Certificates for their roles

- User can get own role certificates via the Web (G³)
- No LRA is involved, just the token, the Pin and Role (G^3)
- » Major savings in travel, LRA time, User time
- Existing private key is RESIGNED into a role Certificate (G3)
- Unique process means its safe on an untrusted workstation (G3)



☐ Users will have many, many badges and certificates

- A different badge is required on the **(Interpret**) and
- Only 3.1M users will have CAC, 1M will have something else
- Many users will have a CAC, one or more organizational badges
- » Typical user may have four badges
- By the nature of the token, each badge has multiple certificates
- Personal Identity sponsored by the badge issuer (CAC model)
 - Personal Encryption certificate for primary email
- Personal Encryption certificates for secondary email addresses
- » Role certificates for within the organization for signing
- Role certificates for within the organization for encryption for role
- › Historical encryption certificates
- Typical badge may have from 1 to 8 certificates

TRW

□ TRW structures the KMI directory for GIG/PKI

- Directory is substructured by sponsor (G3)
- Recognizes a person can have many sponsors (CAC, 22 agencies)
- Directory is substructured by type of sponsored entity (G3)
- Employees, partners, customers, Servers, Roles, Groups
- Directory is substructured by Entity Identity (G3)
- » Each Sponsor supplies unique World Wide ID (WWID)
- Prevents identity theft
- Directory is substructured by Token (G³)
- » Recognizes multiple badges per identity
- » Provides for temporary badges, prevents badge theft
- » Provides for multiple classification levels
- Directory is substructured by Certificate (G3)

Recognizes many certificates/keys per token

- » Allows autorevoke of lost token
- TRW approaches uses replication for GIG (G3)

TRW PROPRIETARY

. 1

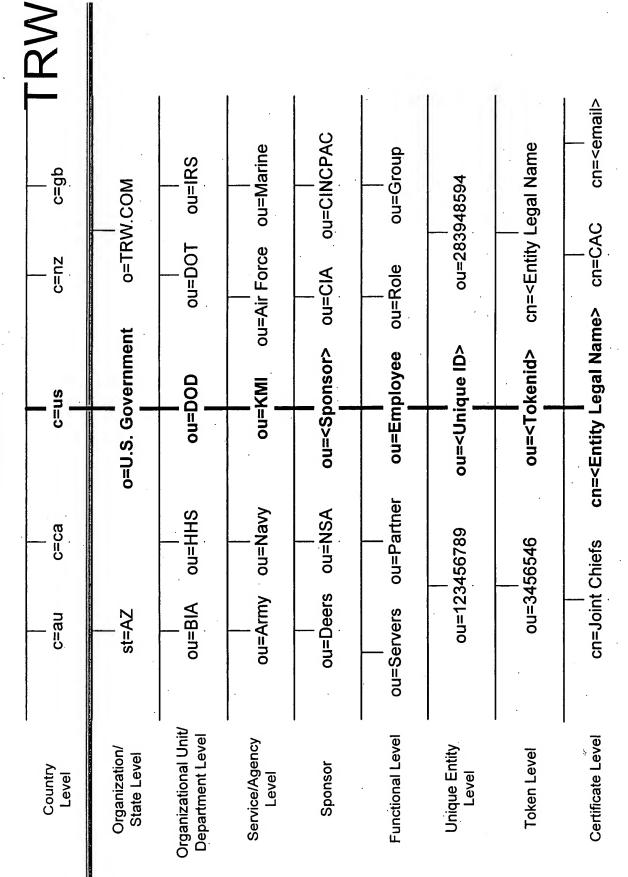
1 1

4 1

! !

1

•



TRW PROPRIETARY

The G³ Summary - User

From the User Viewpoint - Its just a badge

- a badge is issued with a PIN
- » Used to sign things and visit web pages that's all that is needed
- » Never visit the badge office unless the badge expires or is lost
- Office Worker a badge is issued with a PIN
- Used to sign things and visit web pages
- Also used to encrypt files and emails self handled
- Recovery of historical files self handled
- » Never visit the badge office unless the badge expires or is lost
- Organizational Worker a badge is issued with a PIN
- Used to sign things and visit web pages
- Also used to encrypt files and emails self handled
- » Recovery of historical files self handled
- » Issuance and recovery of role keys self handled
- Never visit the badge office unless the badge expires or is lost

□ Replace the badge every 3 years, its easy

TRW PROPRIETARY

13

The G³ Summary - 22 Agencies

TRW

1]

□ Each Agency controls its badging system

- Identity totally under the control of the sponsor
- » Identity certificates automatically issued
- Badging under the control of the sponsor
- PKI entities under the control of the sponsor
- » Employees, Partners, Customers, Servers, Roles, Groups
- Agency issues their own tokens
- No additional operational costs at the badging office
- Automated E-Forms system for creation of PKI entities
- Easily tailored to Agency requirements
- **Encryption and Role certificates Self Handled**
- □ Full Control of their entities
- Minimum Cost to maintain full security
- 1 Minimal disruption and training

The G3 Summary - Carl and Killi

TRW

☐ The The This - a high security underpinning for KMI

- Primary identity key-pair generated at a trusted workstation
- Private identity key is generated on the token itself, never leaves
- Happens invisibly during badge generation
- Full Face-to-Face and ink signature collected as part of badging
- Additional identities, such as roles, are resigns of private key
- » This can be done safely on untrusted workstations
- » A major advantage for the next generation KMI
- Encryption certificates are generated at the central facility
- FIPS-140-3 level key generates assure the highest quality keys
 - Keys are returned wrapped in the public key of the owner
- Can only be recovered on a specific token, by a specific user
- » Fully secured even on an untrusted workstation
- » Key recovery mechanism is fully automated for self recovery

High Security and Low Cost, a win for KMI

TRW PROPRIETARY

15

Improving Key Generation & Delivery Processes for The Smart Cards

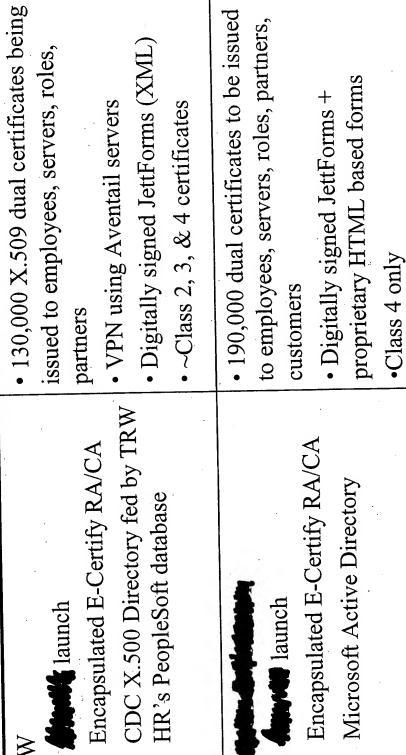
TRW Our PKI Background - Pilots (2)

 1000+ X.509 signing certificates issued to employees, servers, roles, customers VPN using Aventail servers Employees authenticate from home using Aventail clients 	 200+ signing certificates for employees, servers Signatures for HTML based forms 7 separate pilots for PK enabled applications
TRW Pilot Sep 99 – Jan 01 Netscape CMS CDC X.500 Directory fed by TRW HR's PeopleSoft database	Apr 00 – Jan 01 E-Certify RA/CA Isode X.500 Directory

it Plans

TRW

nc	• 1 issi pai • \cdot • \cdot
roduction PKI Rollou	RW Encapsulated E-Certify RA/CA CDC X.500 Directory fed by TRW HR's PeopleSoft database



TRW Recent Insights, Lessons Learned

- If tokens have a digital identity, great things are possible
- Discrimination between Class 2, 3, 4 certificate stores
- Recognition of TRW versus non-TRW tokens
- Secure, high integrity data path from CMS all the way to the token over any non-secure network, through un-trusted workstation
- Greatest long term cost savings will come from transition to signed XML forms, automated workflows
- Eliminate most paper forms and people to push them
- First example is reduction of labor for PKI O&M
- Tighter security, accountability, auditability
- Non-repudiation if forms and data signed digitally
- Data integrity if forms serialized, auto-filled, and signed by CMS

[R&D Design Goals

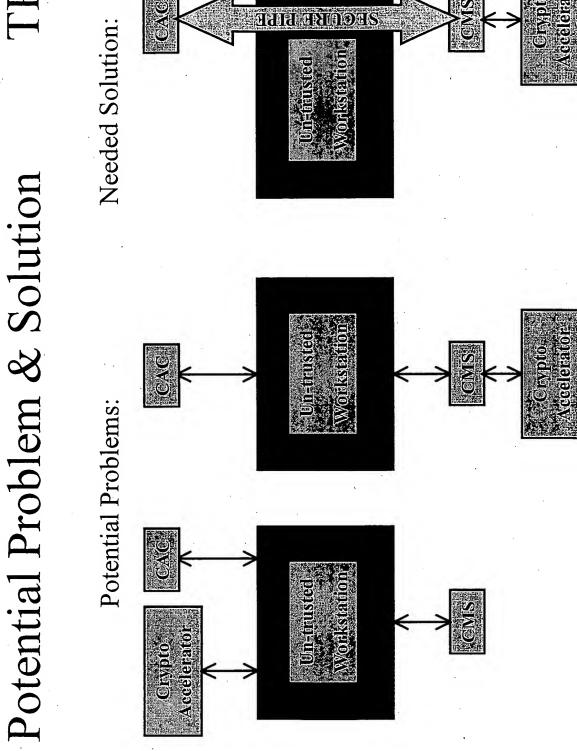
- Improve speed, security, & data integrity of key generation and key distribution
- Reduce number of potential points of failure
- Reduce complexity of LRA workload
- Reduce overall life cycle cost
- Eliminate need for trusted LRA workstations
- obtain additional certificates (roles, encryption...) Eliminate need for personnel to re-visit LRA to
- Simplify processes for historical recovery of encryption certificates

Rationale

TRW

- trusted communications between workstation & Smart Card Need for trusted LRA workstations driven by need for
- Potentially simple solution:
- Validate existing standards-based way to give each Smart Card a private key for unwrapping encrypted private keys & certificates
- Have CA retain each card's corresponding public key in protected database or directory branch
- Have CA wrap (encrypt) and sign all certificates intended for storage on a Smart Card using that card's public key
- Requires only 2 trusted Smart Card key generation systems world-

TRW

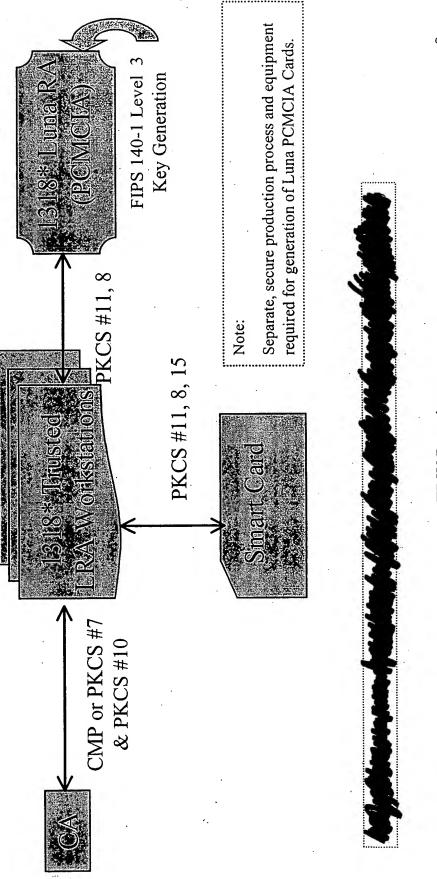


TRW Proprietary

01/04/2001

Technical Approach #1

TRW



01/04/2001

TRW Proprietary

Pros/Con for Approach #1

TRW

- Faster, more robust key generation
- > Sample costs for RAPIDS based CAC
- o 1318 trusted workstations/environments for LRAs
- o 1318 Chrysalis Luna PCMCIA Cards (~ \$28M)
- o Processes/facility for Luna PCMCIA Card generation
- security link (1318 potential points of compromise) LRA is still a critical PKI component and weakest
- o Higher skills required than shown by current Class 3 PKI's E-1s and foreign nationals
- "Non-repudiation" of private key could face legal challenge since not generated on Smart Card

There are four combinations of privacy modes and integrity modes. The privacy modes use encryption to protect personal information from exposure, and the integrity modes protect personal information from tampering. Without protection from tampering, an adversary could conceivably substitute invalid information for the user's personal information without the user being aware of the substitution.

The following are the privacy modes:

- Public-key privacy mode: Personal information is enveloped on the source platform using a trusted encryption public key of a known destination platform (see Section 3.3). The envelope is opened with the corresponding private key.
- Password privacy mode: Personal information is encrypted with a symmetric key derived from a user name and a privacy password, as in [15]. If password integrity mode is used as well, the privacy password and the integrity password may or may not be the same.

The following are the integrity modes:

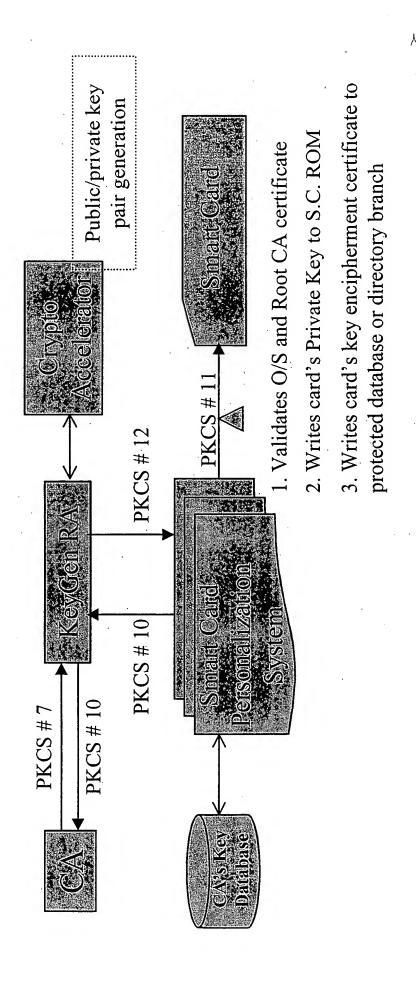
signature key. The signature is verified on the destination platform by using the Public-key integrity mode: Integrity is guaranteed through a digital signature on the contents of the PFX PDU, which is produced using the source platform's private corresponding public key (see Section 3.4).

(MAC) derived from a secret integrity password. If password privacy mode is used as well, Password integrity mode: Integrity is guaranteed through a message authentication code the privacy password and the integrity password may or may not be the same.

Technical Approach #2

TRW

1



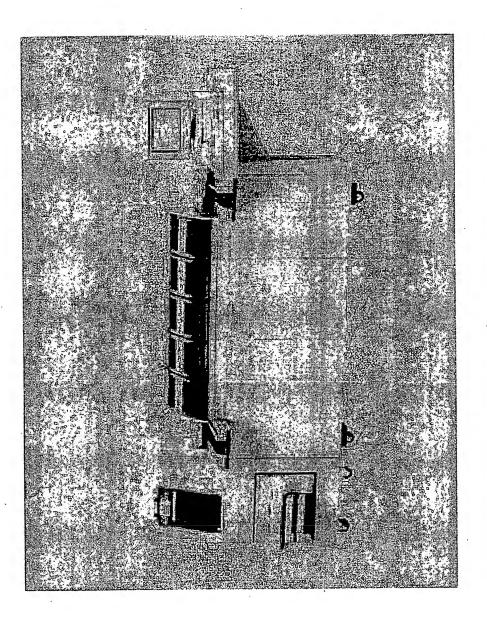
Technical Points - Approach #2

TRW

- PKI Smart-Card Key Generation System (S-CKGS) would be installed in PKI containment facilities
- S-CKGS validates O/S load and Root CA certificate for Smart Card
- S-CKGS generates unique 1024 bit key pair for each serialized Smart-Card using FIPS 140-1 Level 3 crypto accelerator
- CA signs card's public key into Key Encipherment certificate with OU=<Smart Card serial number>
- Smart Card's certificate (public key) written to protected PKI database (only CA has access to public keys for Smart Cards)
- S-CKGS writes card's private key to Smart Card ROM
- DataCard 9000 can perform this process at 900 cards per hour

DataCard 9000

TRW

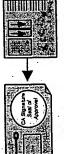


CONOPS for Smart Card Based PKJ

1. Smart cards are drop-shipped to **CMS facility**

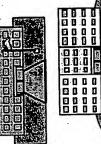


loaded with unique key wrapping keys 2. Smart cards are



3. Secret key for each smart card is saved

 TRW





badging Facility,

shipped to badging

facilities

4. Smart cards

credentials presents

5. User visits

Officer reviews credentials 6. Badging



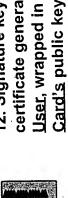
User - previous badges redundant badge for are revoked/expired 8. CMS checks for



user's organizational filled at CMS from 9. E-Form is auto database



certificate generated for User, wrapped in Smart 12. Signature key and



validates Badging

review data against

E-Form & submits

credentials, signs

10. Badging Officer

id, Smart card ID, &

7. Badging Officer

signs request for

E-form with user

organization code

11. CMS facility

gets E-Form &

Officer signature

keys & certificates encryption, role 15. User gets at own desk



assigned to user can 14. Only smart card

unwrap the private

keys

18. Massive reduction with superior security in operational costs



Officer gets keys

13. Badging

16. User never visits badge within seconds & certificate



expired badge or termination

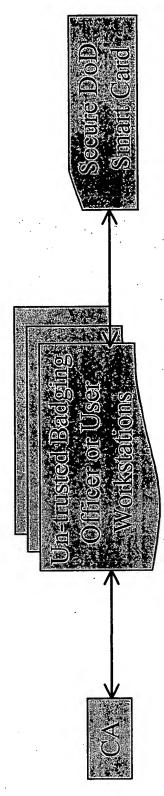
01/04/2001

office except for lost or

minimal PKI training 17. Badging Officer operating system, needs no trusted



TRW Proprietary



Issuing the User's X.509 Signing Certificate:

- Badging Officer uses un-trusted workstation to bind specific Smart Card serial number to specific user ID for that C/S/A.
- CA wraps user's private key and signing certificate in public key of the specific Smart Card, Integrity Mode of PKCS #12. Private key is marked as non-exportable. User bound to that signs the wrapped package, and sends via Public Key Privacy Mode and Public Key Smart Card ID in CMS.

All subsequent Role, Group, and Encryption certificates:

- Badging Officer not required; users can securely obtain all other certificates from any untrusted PC or workstation.
- CA wraps each new certificate using the user's Smart Card's public key and then signs the

Concept for Secure Forms Processing

- XML based forms from JettForms, PureEdge
- Badging Officer authenticates to RA/CA server
- Badging Officer requests badge issuance form for <User D>, <C/S/A ID>, and <Smart Card serial number>
- CMS retrieves that C/S/A's form, assigns serial number to database or directory, signs the form, logs it to audit trail, form, auto-fills the user's data from the authoritative & issues it to Badging Officer
- Badging Officer and user validate data
- Badging Officer signs & submits finalized request

_

- configuration DataCard 9000 can process 900 DataCard engineers estimate that a minimum Smart Cards per hour
- 7 parallel paths at 28 seconds per Card
- 2 sites can process 1800 cards per hour

per 2 machines (versus ROM ~

Eliminates need for Badging Officers to have trusted workstations (\$\$)

Benefits

- Fewer points of vulnerability; lower skill levels
- Much faster key pair generation times
- Eliminates need for 1318 remote crypto accelerators to generate key pairs (\$\$)
- LRA becomes simply a badging person (notary)
- "I swear that I validated J. Doe's credentials and issued badge #130440 to him/her."
- After initial face-to-face, no need for Badging Officer for other certificate requests (\$\$)
- Smart Cards become integral part of central CMS
- Smart Card Only CMS can load a certificate on any

Assess potential impacts to **The** Smart Card: Kecommendations

- Verify whether support for PKCS #12 is requirement under Smart Card contract(s). If so,
- Require use of Public Key Privacy and Public Key Integrity exchange modes
- Remove support for Password Privacy and Password Integrity exchange modes from CAC S/W
- Note: This prevents a denial of service attack on the Smart Card.
- Assess impact of storing private key on Smart Card
- Verify whether Root CA certificate is already on CAC
- Validate potential for cost savings



ee Instructions on Website: h	ittp://we	ephost.ii w				aga dili						
SE MONUCUONS ON TROPINS.				alim			Date	e: 2/19	9/01			
itle of Invention: PKI Token Is	ellance	and Bind	ling Pro	cess								
itle of Invention: PKI Token is	Suarroc	S dila Silia										
	. '		•		!d.s.\$0	inina ir	vento	rshipl				
nventor(S) [See instructions Note: to add more inventors. p	s on W	ebsite for	r assisi	ance	in dete r the las	t entry in 1	the last	column	to ins	ert a ne	w row.)
Note: to add more inventors, p	please	press the	IADK	y arte	. (10 10	TRW		1				•
		Badge	Divisio	on (ccc	Statio		Exten			diate Si	upervis
full Name (No Initials)		150135	IS.		KLB	FP1/416	35	3-502		Bob L		
Kenneth Wagner Aull	1	130440	IS	3	KLC	FP1/416	35	3-561	8	Kathy	McLe	rnon
Thomas Carroll Kerr Type (NMI) if you have no mid	Idlo par	me Pleas		if vou	are a co	nsultant.						
	T Tal	Other	Str	ate	Zip Co	de	Home	Phone		Social	Securit	y Numb
Iome Address	Fair	City	VA		2203					7		a ·
Ken Aull, 5364 Lake	Fair	IdX				-0				-		È
Normandy Ct Tom Kerr, 5348 Black	Fair	fax	VA		2203	2						
Oak Dr	<u> </u>	<u> </u>			<u> </u>							
No P.O. Boxes)												
Date of First Written Descript	tion of t on and	the Inventi Indicate V	ion: Where L	.ocated	d:							
Conception of Invention Date of First Written Descript Identify the Written Description "Card Generation Scheme	on and	Indicate V	Vhere L	ocated	d:						Defense	
Date of First Written Descript	on and es.ppt"	Indicate V	Vhere L	ocated	d:	To Who	om:	<u> </u>	Mary [Dixon, ower D	Defens ata Ce	se nter
Date of First Written Descript Identify the Written Description "Card Generation Scheme Date of the First Oral Disclos	on and es.ppt"	Indicate V	Vhere L	.ocated	d:			<u> </u>	Mary C	wer D	Defens ata Ce	se nter
Date of First Written Descript Identify the Written Description "Card Generation Scheme	on and es.ppt"	Indicate V	Vhere L	ocated 165N	d:	Presen	t Locati	ion: <u>F</u>	/lanpo	wer D	Defens ata Ce	se nter
Date of First Written Descript Identify the Written Description "Card Generation Scheme Date of the First Oral Disclose Date of First Drawings:	on and es.ppt"	Indicate V	Vhere L	ocated 165N	d:	Presen Presen	t Locati t Locati	ion: <u>F</u>	/lanpo	wer D	Defens ata Ce	se nter
Date of First Written Descript Identify the Written Description "Card Generation Scheme Date of the First Oral Disclos Date of First Drawings: Date of First Sketches:	on and es.ppt" sure:	Indicate V	Vhere L	ocated 165N	d:	Presen	t Locati t Locati	ion: <u>F</u>	/lanpo	wer D	Defens ata Ce	se nter
Date of First Written Description Identify the Written Description "Card Generation Scheme Date of the First Oral Disclos Date of First Drawings: Date of First Sketches: Date of Formal Drawings, if	on and es.ppt" sure:	Indicate V	Where L	165N		Presen Presen Presen	t Locati t Locati	ion: F	P1/4	wer D	Defens ata Ce	se nter
Date of First Written Description Identify the Written Description I'Card Generation Scheme Date of the First Oral Disclose Date of First Drawings: Date of First Sketches: Date of Formal Drawings, if	on and es.ppt" sure:	Indicate V	Where L	165N		Presen Presen Presen	t Locati t Locati	on: <u>F</u> ion: _ ion: _	<u> 1anpc</u> -P1/4	ower D	ata Ce	nter
Date of First Written Description Identify the Written Description "Card Generation Scheme Date of the First Oral Disclos Date of First Drawings: Date of First Sketches: Date of Formal Drawings, if Construction And Test	on and es.ppt" sure:	Indicate V	Where L	165N	on box	Present Presen	t Locati t Locati	on: <u>F</u> ion: _ ion: _	<u> 1anpc</u> -P1/4	wer D	ata Ce	nter
Date of First Written Description Identify the Written Description "Card Generation Scheme Date of the First Oral Disclos Date of First Drawings: Date of First Sketches: Date of Formal Drawings, if	on and es.ppt" sure:	Indicate V	Where L	165N	on box	Presen Presen Presen	t Locati t Locati t Locati checked	on: <u>F</u> ion: ion:	Manpo P1/4	ower D	ata Ce	nter
Date of First Written Description Identify the Written Description "Card Generation Scheme Date of the First Oral Disclos Date of First Drawings: Date of First Sketches: Date of Formal Drawings, if Construction And Test	on and es.ppt" sure:	Indicate V	Where L	165N	on box	Presen Presen Presen	t Locati t Locati t Locati	on: <u>F</u> ion: ion:	Manpo P1/4	ower D	ata Ce	nter
Date of First Written Description Identify the Written Description I'Card Generation Scheme Date of the First Oral Disclose Date of First Drawings: Date of First Sketches: Date of Formal Drawings, if Construction And Test Invention Simulated?	on and es.ppt" sure:	located in	where L	165N	on box	Present Presen	t Locati t Locati t Locati checked	on: <u>F</u> ion: _	Manpo P1/4	ower D	ata Ce	nter
Date of First Written Description Identify the Written Description Card Generation Scheme Date of the First Oral Disclose Date of First Drawings: Date of First Sketches: Date of Formal Drawings, if	on and es.ppt" sure:	Indicate V	where L	165N	on box	Present Presen	t Locati t Locati t Locati checked Date:	on: <u>F</u> ion: _	Manpo P1/4	ower D	ata Ce	nter
Date of First Written Description Identify the Written Description Card Generation Scheme Date of the First Oral Disclose Date of First Drawings: Date of First Sketches: Date of Formal Drawings, if Construction And Test Invention Simulated?	on and es.ppt" sure:	located in	where L	165N	on box	Present Presen	t Locati t Locati t Locati checked Date: /hom:	on: <u>F</u> ion: _	Manpo P1/4	ower D	ata Ce	nter
Date of First Written Description Identify the Written Description "Card Generation Scheme Date of the First Oral Disclos Date of First Drawings: Date of First Sketches: Date of Formal Drawings, if Construction And Test Invention Simulated? Invention Modeled?	on and es.ppt" sure:	res or No-Yes	rhere L	e click	on box	Present Presen	t Locati t Locati t Locati checked Date: /hom:	on: <u>F</u> ion: _	Manpo P1/4	ower D	ata Ce	nter
Date of First Written Description Identify the Written Description "Card Generation Scheme Date of the First Oral Disclost Date of First Drawings: Date of First Sketches: Date of Formal Drawings, if Construction And Test Invention Simulated? Invention Modeled?	on and es.ppt" sure:	res or No-Yes	rhere L	e click	on box o 🛭	Present Presen	t Locati t Locati t Locati thecked Date: /hom: Date: Vhom:	ion:	Manpo P1/4	ower D	ata Ce	nter
Date of First Written Description Identify the Written Description "Card Generation Scheme Date of the First Oral Disclos Date of First Drawings: Date of First Sketches: Date of Formal Drawings, if Construction And Test Invention Simulated? Invention Modeled?	on and es.ppt" sure:	res or No-Yes	rhere L	e click	on box o 🛭	Present Presen	t Locati t Locati t Locati thecked Date: /hom: Date: Vhom:	on: <u>F</u> ion: _	Manpo P1/4	ower D	ata Ce	nter

Obtain All Signatures	Date:	Inventor:	Date:	Inventor:	Date:
	Date:	Inventor:	Date:	Inventor:	Date:
nventor: Witnessed, Read and	Understood by:	Witness:	Date:	Supervisor:	Date:

بر IR&D project بر	· . 	•		
Invention Successfully Tested?	Yes 🌪 No 🖣	Date:		
·		by WHOIH.		
Use Or Offer For Sale (Must be C	Completed)			
Was Invention the Subject of Comm		No 🗌	By Whom: Ken Aull	
(Commercial Activity Means External to	TRW and Includes Activity	with the Government)	Date:	
(Commorcial Views)				
If Yes (A) Date of First Execute	d Sales Contract:			·
(B) Identify First Sales C	ontract No.:		-0	
(C) Date Of First Deliver	y To Customer:			
Was Invention Described in a	Yes	No 💮	Date:	
Proposal? Was a Description of the Invention	Yes 🥌	No 🎩	Date:	
Provided to the Government? Was a Description of the Invention	Yes 💮	No 🤚	Date:	
Provided to a Commercial Custom		No 🌦	Date:	
Was a Description of the Invention Provided as Part of an On-going Contract?	res 💮			100
If you answered YES to any of the	above questions, please p	provide a copy of the	e material which included	the
description.			pected Date:	
Is it anticipated that an activity will occur soon? Please provide the	Yes 💮	No 🛖 EX	Decled Balc.	
appropriate information above and enter expected date.		•		·
		-		
Publication (Publication means	inted and distributed	outside TRWI (Mus	st be Completed)	
Publication [Publication means Has a Description of the Invention				•
If Yes, <i>Provide Copy</i> and Identify	Deell Fublished: 103 5	werpoint briefing t	itled "Improving Key G	eneration &
Delivery Processes for	mart Cards"		•	
If The Invention Has Been Describ Customer, Date, and No.	bed in a Customer Report,	Provide Copy and	Identify the Customer Re	eport by
Did the Customer Report Have a	TRW Proprietary Legend?		Yes 👚	No 🥌
Has the Invention Been Describe			Yes 🌎	No 🧼
	er a Confidential Disclosur		Yes	,
	erson(S), Their Employers		e of Disclosure:	
1	. <i>.</i>			
(Obtain All Signatures Before Sensitiventor: Date:	Inventor:	Date:	Inventor:	Date:
inventor.				
Inventor: Date:	Inventor:	Date:	Inventor:	Date:
Witnessed, Read and Understood	by: Witness:	Date:	Supervisor:	Date:

(Obtain All Signatures Bet	rore Senain	g to Paterit Couriser)		1	Date:
Inventor:	Date:	Inventor:	Date:	Inventor:	· Date.
Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Witnessed, Read and Un	derstood by	: Witness:	Date:	Supervisor:	Date:

SYSTEMS125 Rev. 05-99

Related Printed Publicatio					4- 011
Identify Any Patents, Printed Analogous Concepts, and P	d Publication Provide Cop	ns, Written Reports, or Provies:	posals That Yo	ou Are Aware Of Relating	to Closely
/					
Identify Any Prior TRW Inve	ntion Disclo	sures Patent Applications	. or issued Pat	tents Relating to the Inven	ition:
Identily Any Phot TRV IIIve	IIIIOII Discio		,		
			٠.	•	
Ken Aull:	4. (3.8)	-t b- Completed)	· · · · · · · · · · · · · · · · · · ·		
Contract or Project Inform			99X637		
The Invention First Conceiv			93/03/		
And Working On: DoD PKI			Title:		
Government Contract of		Ct No.:	Title:		
TRW Funded (IR&D, Bo Project No.:	&P, PM&P)	· .	- IIUC		
			ustomer.	•	ļ
Commercial Contract N					
		s TRW Technical Fellov			
Contract Administrator				4	
The Invention First Constru	icted vvnile (Charging Time to Job No	· ·		
And Working On:			Title:	٠.	
Government Contract of			- Title: —		
TRW Funded (IR&D, B Project No.:	I&P, PM&P)				
	1		customer:		
Commercial Contract N	No.:		,ustorrier		
Other, Explanation:	Dheno	No:			
Contract Administrator	and Phone	NO			
Tom Kerr:			<u></u>		
Contract or Project Infor	mation (Mu	ust be Completed)			
The Invention First Concei			99X637		
And Working On: DoD PK	Marketing	(OITE)			
Government Contract	or Subcontr	ract No.:	Title:		
(Obtain All Signatures Befo	Date:	Inventor:	Date:	Inventor:	Date:
Inventor:	Date.				
Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
		NACH	Detai	Supervisor	Date:
Witnessed, Read and Unde	erstood by:	Witness:	Date:	Supervisor:	Date.

- {	☐ TRW Funded (IR&D, B&P, Project No.:	P())	1	itle:	<u>.</u>	
	Commercial Contract No.:		Cust	omer:		
1	Other, Explanation: TE	DS, an Int	ernal TRW Project spor	sored by Cle	veland	
	Contract Administrator and	Phone No.	4			
	The Invention First Constructed					
	And Working On:					
	Government Contract or Si	ubcontract	No.:	Title:		·
	TRW Funded (IR&D, B&P,	PM&P)	*	Title:		
:	Project No.:					
	Commercial Contract No.:		Cust	omer:		
	Other, Explanation:		·		,	
	Contract Administrator and	i Phone No).:			
l	,			•		
!	Teil Us All About Your Inventi	ion:	·			
	What was the problem or ne	ed that you	u were trying to solve?			
	Conventional Public Key			•		
	member of the enterprise must use a specific "trust degree of specialized knothis process opens up the Tokenizing Officer. This pit up to later repudiation of intensive way of issuing to certificates stored on a total content of the content of the content of the certificates are the content of the content of the certificates are the content of the certificates are the content of the certificates are the c	ted" works bowledge power token a bossibility control control	station to prepare a to pertaining to PKI techr ssignment process to rendangers the integr ate use by a user. The	ken for a us nology. In ac potential tar ity of an ente problem is	er, and typically require Idition to being labor-int npering and mistakes b erprise PKI system, and to establish a less labor	ensive, y the l opens
1						
	Inventive Concept - What is	<u>new,</u> wha	t it <u>does</u> and <u>how</u> it does	it? Seete seeign	ment procedure throug	h a
	The concept allows a Tobasic interface, such as a in assigning a token to a associated public certific token. It binds the certific Directory/database. It sto	a web pa user. It is ate with the lied token ores a rec	ge. It uses an enterprouses the existence of the organization's Directory ID number to a certification of Tokenizing Off	the Token II ctory/Datab ed user ID n icer's signat	y/Database as proof of of of such as a serial numbase as proof of an eligibumber within an organizure in correlation with cr	cer) and ble zation's reation
	of user signature certifica	ate It ner	nerates the user's sign	nna kev and	cennicate in the centra	
••	Certificate Management package so as to preser	ve the va	lidity of non-repudiation	on. The pub	IIC KEY usea must be the	z Key Oi
	the token that has been	assigned	to particular user. Th	e signature	must be of a subordina	te
	(Obtain All Signatures Before S					
	·			Date:	Inventor:	Date:
				Deter	Inventor:	Date:
	Inventor: Da	ite: Ir	nventor:	Date:	mventor.	Dute.
	Witnessed, Read and Underst	cood by: V	Vitness:	Date:	Supervisor:	Date:
		1	•	l ·		

Lertificate Authority traceate to the Root Public Certificate. It the ransmits the user's certificate/private key to the Tokenizing Officer encrypted for use only by the designated token. The system then delivers (stores) the encrypted package to the user's token. The token is the only entity capable of decrypting the certificate/private key. The token validates the signature of the package, unwraps the key and certificate, and stores them so that they are accessible via CAPI or PKCS#11 calls.

Proof of possession is obtained by requiring an initial digital signature. At that point, the certificate is tagged as being activated by publishing of the certificate within the directory.

Invention Description and Operation: (Attach Drawings Or Sketches for Each Embodiment)

A User presents credentials to the Tokenizing Officer, who enters user's ID number, organization, and token ID number into E-form Request web page. The E-form Request is sent to Certificate Management System (CMS), which checks for existing tokens for the user and revokes the certificates contained on the token. The CMS then identifies user's organization and loads an organization-specific E-form. The CMS auto-fills the E-form with data from the user's organization's directory/database and returns the auto-filled E-form to Tokenizing Officer. The Tokenizing Officer compares form data with the user credentials. The tokenizing officer electronically signs the form, and submits it back to the CMS. The CMS facility receives the form and validates the Tokenizing Officer's signature against the certificate recorded by Certificate Authority. Certificate Authority generates the user's key and signing certificate and wraps (encrypts) it using the specified token's public key. This data package is then transmitted to the Tokenizing Officer's workstation, where the Tokenizing Officer stores the data package on the token. The encrypted package contains the user's private key and public certificate. Finally, Tokenizing officer issues token to user. The Tokenizing officer retains a copy of the personally signed form in which the user accepts the token, and all its responsibilities. This meets the requirement for a traceable wet signature to any digital signature, as well as requirements for a "face-to-face", required by most high-trust CMS systems.

Finally, the user must digitally sign the E-Form for final submission to the CMS system. This signature provides proof of acceptance. Upon receiving proof of acceptance, the certificate is published in the directory by the CMS system. A compatible On-Line Certificate Status Protocol (OCSP) responder will then reply to any validation request that the certificate is now valid. The OCSP will reply with a valid response to any certificate which has been published in the directory, and which is not in the Certificate Revocation List (CRL). The OCSP will reply unknown if the CRL is not available, or current, or if the certificate is not published. The OCSP will respond invalid if the CRL indicates that the Certificate for the user has been revoked.

Briefly describe what the prior art taught:									
Obtain All Signatu	res Before Sending	to Patent Counsel)			Date:				
ventor:	Date:	Inventor:	Date:	Inventor:	Date.				
nventor:	Date:	Inventor:	Date:	Inventor:	Date:				
			Date:	Supervisor:	Date:				
litnessed, Read a	and Understood by	Witness:	Date:	·					



What are the advantages to your invention?

The Tokenizing Officer in this system requires no PKI-specific training, but rather needs only to be able to operate a web page like interface. This Tokenizing system transmits the user's signing certificate to the Tokenizing Officer in a form that only the user's designated token can decrypt, securing it from tampering. The Tokenizing Officer's electronic signature is archived to provide an audit trail in the event of signature repudiation questions or issues. These measures decrease the cost for training of Tokenizing personnel, and increase the integrity of the user's signing certificate.

Government, industrial or commercial applications:

What are the current plans, if any, for the concepts discussed in the Invention Disclosure? If none, please so state.

This concept will be suggested to other commercial and government customers as part of TRW marketing activities associated with PKI or other digital signature technologies.

Is there an intended TRW commercial product that will use the concepts in this invention Disclosure?

There is a "product" in the sense that S&ITG will offer at a pre-defined price with a pre-defined schedule a PKI "solution" to both commercial and government customers. That product is still being defined. Multiple divisions are participating in the definition of the product.

If Yes, what is the intended commercial product?

The product is an "e-business" solution that provides digital signatures and paperless workflow to an enterprise.

If Yes, when will the intended commercial product be developed?

Is there an intended TRW generic use for the concepts in this Invention Disclosure?

If Yes, what is the intended generic use?

(Obtain All Signatures Before Sending to Patent Counsel)

Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Witnessed, Read and	I I Understood by:	Witness:	Date:	Supervisor:	Date:

Supplemental One Sheet Description - In Viewgraph Format, Tell Us About Your Invention (To be Used at Invention Evaluation Committee Meeting)

Title: PKI Token Issuance and Binding Process

Summary of Idea:

The process of using a secure electronic system to allow an authorized individual (Tokenizing Officer) within an enterprise to assign a token to a user while eliminating the possibility for compromise of the token generation process.

What Do You Believe is the Innovative Concept:

The innovative concept is that Tokenizing officer functions are reduced to the bare minimum, validating the identity of a user of the system by the comparison of database information with presented credentials. The process of recording a correlation between a token, a user, and all certificates stored on a token is "User ID Binding". This process is initiated when the Tokenizing Officer assigns a token to an entity. Once the entity and the token are bound together in the directory, any certificates (identity or role) that are established on the token (via encrypted download using the Primary Token Identity Certificate) are also bound to the entity. The Certificate subject name (in the directory tree) is designed to bind the identity or role of the user, the identity of the token, and any and all future PKI certificates together.

What is the Closest Prior Art Known to You:

Many territories and the Charles of the Control of

List Competitive Advantages:

Reason Why We Should File a Patent for Your Invention:

Call up 1st down

Law Department

One Space Park Redondo Beach, CA 90278 310.812.4321 E2/6051 310.812.1534 Telecopier 310.812.2687 E-mail: loma.schott@trw.com

April 5, 2001

Donald E. Stout, Esq. Antonelli, Terry, Stout & Kraus, LLP **Suite 1800** 1300 North Seventeenth Street Arlington, Virginia 22209

Subject: TRW Docket No. 15-0251

Last Day to File Application:

Gov't. Contract No.: Restricted

Billing Unit: SITG/IIT-DSO - Billing Code: 312

TRW Docket No. 15-0252 Last Day to File Application:

Gov't. Contract No.: N/A

Billing Unit: SITG/IIT-DSO - Billing Code: 312. 199.40006XDD

TRW Docket No. 15-0254 Last Day to File Application;

Gov't. Contract No.: N/A

Billing Unit: SITG/IS - Billing Code: 312

TRW Docket No. 15-0255

Last Day to File Application: Gov't. Contract No.: N/A

Billing Unit: SITG/IS - Billing Code: 312

TRW Docket No. 15-0256

Last Day to File Application:

Gov't. Contract No.: N/A

Billing Unit: SITG/IS - Billing Code: 312

Dear Don:

Enclosed herewith are copies of the above-referenced invention disclosures. No formal patentability searches will be conducted in these matters.

Donald E. Stout, Esq. April 5, 2001 Page 2

The first draft applications should be submitted to this office no later than **Constitution**. All cases have potential statutory bar dates. TRW Dockets No. 15-0254, 15-0255, and 15-0256 should be filed on the same day. Please follow the new format for preparing the patent applications based on the new Rules and Regulations (see Federal Register/Vol. 65, No. 175/Friday, 9/8/00). The draft applications and drawings should be sent by regular U.S. mail, along with a copy of each on disk.

You should also be aware that all transmittals of drafts and comments should be directed to this office, and not directly between you and the inventor, so that I can keep track of the progress of the preparation. If you need to deviate from any of the above procedures, please contact me immediately.

Attached is a list of standards that we are now requiring for all patent application preparation. Please follow these guidelines.

The transmittal should indicate whether or not there are any statutory bars running of which you are aware, and whether or not there are any impediments to our filing corresponding foreign applications. Your firm is also responsible for informing us if there are any related and/or co-pending applications that are to be filed at the same time.

So that there is no question as to division of responsibilities, this office will be responsible for the preparation of the formal papers (declaration, power of attorney, assignment) and the actual filing of the applications.

I look forward to working with you to obtain the best patent coverage we can for these inventione. If you have any questions concerning these matters, please do not hesitate to contact me.

Lorna L. Schott

Sincerely.

Patent Administrator

/lls

Enclosures

Donald E. Stout, Esq. April 5, 2001 Page 3

PATENT APPLICATION PREPARATION STANDARDS

- The first page of the application should include: Title, Headings for Cross-reference and/or Government clauses, only when applicable (leave out if not applicable), followed by Background, Summary of Invention, etc. Do not include a separate Cover/Title page,
- The header should contain the TRW Docket Number in the upper right hand corner, as well as the Express Mail, mailing language,
- Standard government contract clause (Restricted or Unrestricted) inserted upon first draft, when applicable,
- Specification with claims,
- Drawings prepared in semi-formal format (no shading see Guide for the Preparation of Patent Drawings - Dept. of Commerce),
- Information Disclosure Statement and Form PTO-1449 signed by vou.
- Abstract (no longer than 150 words, not including the title) with reference numerals suitable for filing in foreign jurisdictions,
- Title of patent application on the abstract,
- Draft application on 8 1/2" x 11" bond paper (Please follow the new format as stated in the Rules and Regulations - Federal Register/Vol. 65, No. 175).
- Copy of the application (initial drafts and subsequent drafts) on diskette readable by Microsoft Word running on a P.C. enclosed in a protective cover.
- The transmittal should also indicate whether or not there are: any related cases, statutory bars running of which you are aware, and whether or not there are any impediments to our filing corresponding foreign applications.
- All interviews with inventors should be cleared through this office. Any subsequent interviews, correspondence, or document exchange between you and the inventor should also be directed through this office, as well as copies of all documentation sent to us.

Henry Zykorie

From:

Henry Zykorie

Sent:

Wednesday, April 11, 2001 10:01 AM

To:

'ken.aull@TRW.com'; 'tom.kerr@TRW.com'

Cc:

'Lorna.schott@TRW.com'

Subject:

TRW Docket #15-0254; Our Docket #199.40006 x00

Importance:

High

Good morning:

My name is Henry Zykorie, and I am a patent attorney of the Washington, D.C.area law firm of Antonelli, Terry, Stout & Kraus, LLP. Our law firm has been assigned to draft/file a patent application for one of your recent TRW invention disclosures as identified above.

I would like to arrange a telephone interview with both of you in order to prepare the application. Accordingly, please tell me when will be the best time for me to call you directly to discuss about the application. Also, the following items are very helpful in facilitating discussions of the invention and/or teaching us about the technology to which the invention is related:

- 1) Any prior art articles and/or relevant technical publications relating the general state of the art that you might have considered during conception and preparation of your Invention Disclosure, or of which you are aware including a copy of the PowerPoint publication cited in the Invention Disclosure;
- and 2) A copy of drawings, sketches and/or any text of the invention that you might have prepared for the Invention Disclosure on a floppy disk (this can be helpful for us to prepare informal drawings of the patent application for filling in the U.S. Patent & Trademark office).

Further, it is recommended that you facsimile (fax703/312-6666) or mail such materials to us in advance of any telephone conference, as it is helpful if we can both access and discuss similar materials during the telephone conference.

I would like to start working on the patent application as quickly as possible, so your promptness to confirm the above schedule would be greatly appreciated. I look forward to working with you on this patent application.

Best regards,

Henry
Henry M. Zykorie
Antonelli, Terry, Stout & Kraus LLP
1300 North Seventeenth Street
Suite 1800
Arlington, Virginia 22209
(tel) 703 312-6634
(fax) 703 312-6666
e-mail: hzykorie@antonelli.com

Henry Zykorie

From: Sent: Tom Kerr [Tom.Kerr@trw.com] Thursday, May 03, 2001 8:09 AM

To:

Henry Zykorie

Cc:

'Ken Aull'; 'Lorna.schott@TRW.com'

Subject:

Re: TRW Docket #15-0254; Our Docket #199.40006 x00



Card Generation

Schemes.ppt Ken and I are done with the proposal that we have worked for the past 8

I'm attaching the Powerpoint presentation cited in the invention disclosure.

Will forward additional documents and drawings that we prepared earlier for

these dockets.

Unfortunately, the company has taken 4 related PKI dockets and given them out to four different persons to finalize the patent applications. FYI - there are 12 previous PKI patent applications filed last year by TRW - upon which this builds.

Give us a call any time when you return to the office.

Tom Kerr TRW Systems 1 Federal System Park Drive Mail Stop: FP1/4165 Fairfax, VA 22033

703-803-5618

Henry Zykorie wrote:

- > Hi again-
- > Just a reminder that I had yet to receive a response to my April 11,
- > e-mail noted below.
- >
 > I await your response noting that I will be out of the office from

Thursday,

Accordingly, please reply

as soon

- > as possible!
- > Regards,
- > Henry

1

1 1

- > Henry M. Zykorie
- > Antonelli, Terry, Stout & Kraus LLP
- > 1300 North Seventeenth Street
- > Suite 1800
- > Arlington, Virginia 22209
- > (tel) 703 312-6634
- > (fax) 703 312-6666
- > e-mail: hzykorie@antonelli.com

DONALD R. ANTONELLI DAVID T. TERRY MELVIN KRAUS WILLIAM I. SOLOMON* GREGORY E. MONTONE RONALD J. SHORE DONALD E. STOUT ALAN E. SCHIAVELLI JAMES N. DRESSER CARL I. BRUNDIDGE* PAUL J. SKWIERAWSKI* ROBERT M. BAUER

RANDALL S. SVIHLA HUNG H. BUI* GEORGE N. STEVENS* FREDERICK D. BAILEY DAVID C. OREN RALPH T. WEBB*

*ADMITTED OTHER THAN VA

LAW OFFICES

ANTONELLI, TERRY, STOUT & KRAUS, LLP

SUITE 1800 1300 NORTH SEVENTEENTH STREET ARLINGTON, VIRGINIA 22209

June 22, 2001

OF COUNSEL HENRY M. ZYKORIE* ROBERT F. GNUSE

PATENT AGENT LARRY N. ANAGNOS

TELEPHONE (703) 312-6600 FACSIMILE (703) 312-6666

WRITER'S DIRECT EMAIL hzykorie@antonelli.com

Lorna L. Schott Patent Administrator TRW Inc. One Space Park Redondo Beach, CA 90278

Re: DRAFT APPLICATION of TRW-150254

Dear Lorna:

We have completed the preparation of the above-identified application and enclose a paper copy of the application and drawings as well as a disc containing the application. Please advise if you need in changes made to the application. We have forwarded this via Federal Express but have not billed you for those charges.

Very truly yours,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Henry M. Zykorie

HMZ:dmw



TRW Inc.

Law Department One Space Park Redondo Beach, CA 90278 310.812.4321 Direct Dial No. 310.812.1534 Telecopier 310.812.2687 Building E2/6051

October 18, 2001

Henry M. Zykorie, Esq. Antonelli, Terry, Stout & Kraus, LLP 1300 North Seventeenth Street, Ste. 1800 Arlington, VA 22209

40006X00

Subject:

TRW Docket No. 15-0254; Your File No. 199.40006X00

Title: PUBLIC KEY INFRASTRUCTURE TOKEN ISSUANCE

AND BINDING

√ Dear Henry:

Enclosed please find the inventor's first review comments in connection with the above-referenced application. TRW will prepare the formal drawings. Please note there is a incorporate these changes and return the revised application to me and include an electronic version on disk in Word 6.0 for the PC.

For your convenience, I have also enclosed the disk submitted with the original draft application.

Thank you for your attention in this matter.

Sincerely,

Lorna L. Schott

Patent Administrator

/mlb ·

Enclosures

DONALD R. ANTONELLI MELVIN KRAUS WILLIAM I. SOLOMON* GREGORY E. MONTONE RONALD J. SHORE DONALD E. STOUT ALAN E. SCHIAVELLI JAMES N. DRESSER

LAW OFFICES ANTONELLI, TERRY, STOUT & KRAUS, LLP

SUITE 1800

1300 NORTH SEVENTEENTH STREET ARLINGTON, VIRGINIA 22209 October 26, 2001 OF COUNSEL
DAVID T. TERRY
HENRY M. ZYKORIE*
ROBERT F. GNUSE
HAROLD A. WILLIAMSON*

PATENT AGENT LARRY N. ANAGNOS

> TELEPHONE (703) 312-6600 FACSIMILE (703) 312-6666

EMAIL email@antonelli.com

RANDALL S. SVIHLA HUNG H. BUI* GEORGE N. STEVENS* FREDERICK D. BAILEY DAVID C. OREN RALPH T. WEBB*

CARL I. BRUNDIDGE*

PAUL J. SKWIERAWSKIP ROBERT M. BAUER

*ADMITTED OTHER THAN VA

Lorna L. Schott
Patent Administrator
TRW Inc.
One Space Park
Redondo Beach, CA 90278

Re: TRW Docket No. 15-0254 – Our File No. 199.40006X00 Title: PUBLIC KEY INFRASTRUCTURE TOKEN ISSUANCE AND BINDING

Dear Lorna:

Thank you for your letter of October 18, 2001. We have made the requested revisions to the application and enclose the same as a paper copy as well as on disc.

Please advise if you have any further questions in connection with this application.

Very truly yours,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

By:_____Henry M. Zykorie

HMZ:dmw Enclosures

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

□ BLACK BORDERS
□ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
□ FADED TEXT OR DRAWING
□ BLURRED OR ILLEGIBLE TEXT OR DRAWING
□ SKEWED/SLANTED IMAGES
□ COLOR OR BLACK AND WHITE PHOTOGRAPHS
□ GRAY SCALE DOCUMENTS
□ LINES OR MARKS ON ORIGINAL DOCUMENT
□ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
□ OTHER:

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.